ФІШИНГОВІ АТАКИ. ЗАСОБИ БОРОТЬБИ З НИМИ

Мартіросян М.К., Князєв І.А.
Науковий керівник – ***Новожилова М.В., д-р фіз.-мат. наук, професор,***

Фішинг – це вид інтернет-шахрайства, яка полягає в крадіжці конфідейційних даних користувачів. Основним завданням фішинг шахрає є отримання вашого логіна та пароля від певного сайту. У 2016 році зафіксовано зниження частки масової розсилки фішингових листів. Це пов'язано з тим, що великі компанії приділяють все більше уваги захисту конфіденційних даних користувача. Специфікою фішингу є те, що жертва шахрайства надає свої конфіденційні дані добровільно. Для цього зловмисники оперують такими інструментами, як фішингові сайти, E-mail розсилка, фішингові landing page, спливаючі вікна, таргетована реклама.

Приклади схем інтернет-фішингу:

1. Шахраї створюють електронні листи з підробленим рядком "Mail From:", використовуючи недоліки в поштовому протоколі SMTP. Коли відвідувач відповідає на фішингові повідомлення, лист з відповіддю автоматично пересилається шахраям по електронній пошті.
2. Фіктивні благодійні організації, які звертають з проханням про пожертвування.
3. Створення фішингових інтернет-магазинів (товари продаються за вигідними цінами або з великими знижками. Це приваблює відвідувачів і вони дають дані своїх банківських карт, не підозрюючи, що стають жертвою шахрайства).
4. Розсилка підроблених електронних листів, з проханням підтвердити логін і пароль

Як розпізнати фішинг: на електронну пошту приходить лист, який починається словами «Вітаємо! Ви виграли ... ". Вам повідомляють про перемогу в розіграші або лотереї, і щоб отримати приз, потрібно лише авторизуватися, залишивши на чужому ресурсі свої особисті дані.

Засоби боротьби з фішинговими атаками:

1. Встановити якісний антивірус. Як правило, у всіх сучасних антивирусів передбачений захист від шпигунських і шкідливих програм.
2. Завжди звертайте увагу на дизайн сайту: якщо сайт здається дивним, недопрацьованим або викликає якісь підозри, то існує ймовірність, що це фішинговий сайт.

3. Звертайте увагу на адресний рядок: незначні зміни в електронній адресі можуть привести вас на абсолютно інший сайт (наприклад, замість mail.ru може бути meil.ru, а замість vk.com - vk.co або vka.com).
4. При відвідуванні банківських сайтів, стежте, щоб було встановлене захищене з'єднання https.
5. Листи з невідомих адрес, які «тиснуть на емоції» або носять екстрений характер, повинні в першу чергу викликати підозри. Листи, які починаються з таких заяв, як «Ваш профіль буде заблоковано!» Або, навпаки, оголошують вам про великий виграш, в більшості випадків є шахрайськими.
6. Будьте обережні заходячи на банківські веб-акаунти через точки доступу громадського Wi-Fi.
7. Якщо виявили фішинговий лист нібито від відомої вам компанії або сервісу, повідомте про це у відділення цієї компанії.

Не так давно одна з британських компаній, що спеціалізується на захисті від шахрайства в інтернеті, провела цікавий експеримент. Відвідувачам кав'ярні пропонували безкоштовну каву в обмін на лайк корпоративної сторінки закладу в Facebook. Поки відвідувач робив замовлення, співробітники аналізували профіль людини і дізнавалися про нього безліч особистої інформації. Поки готувалася кава, бариста встигав «вивалити» на приголомшену людину інформацію про його день народження, імена батьків, освіту, віросповідання і тому подібне. І все це завдяки всього-на-всього одного лайку! Таким інтерактивним способом компанія акцентувала увагу громадян на необхідність захисту своїх персональних даних.

Пропонуємо, один із засобів боротьби з фішинговими атаками. AdBlock - це розширення для веб-браузера. Воно не тільки заблокує зайву рекламу, а ще попередить про неперевірені сайти. Adblock блокує HTTP-запити відповідно з адресами джерела і може блокувати різні типи елементів сторінки.

ВИКОРИСТАННЯ SQL-ЗАПИТІВ ДЛЯ ОТРИМАННЯ ІНФОРМАЦІЇ З СИСТЕМИ MOODLE

Лє В`єт Ань
Науковий керівник – ***Бочаров Б.П., канд. техн. наук, доцент***
(Харківський національний університет міського господарства імені О.М. Бекетова)

В системі дистанційного навчання Харківського національного університету міського господарства встановлено спеціальний модуль